ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-13-095-02 ROCKWELL AUTOMATION FACTORYTALK AND RSLINX MULTIPLE VULNERABILITIES

April 5, 2013

OVERVIEW

Researcher Carsten Eiram of Risk Based Security has identified multiple input validation vulnerabilities in Rockwell Automation's FactoryTalk Services Platform (RNADiagnostics.dll) and RSLinx Enterprise Software (LogReceiver.exe and Logger.dll). Rockwell Automation has produced patches that mitigate these vulnerabilities, and released the patches April 5, 2013. Rockwell Automation has tested the patches to validate that they resolve the vulnerabilities.

These vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

The following FactoryTalk Services Platform and RSLinx Enterprise products are affected:

CPR9,

CPR9-SR1,

CPR9-SR2,

CPR9-SR3,

CPR9-SR4,

CPR9-SR5

CPR9-SR5.1, and

CPR9-SR6.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

IMPACT

Successful exploitation of these vulnerabilities may result in a DoS condition to the services, service termination, and the potential for code injection.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

Rockwell Automation provides industrial automation control and information products worldwide, across a wide range of industries.

The affected product, FactoryTalk Services Platform (FTSP), shares data throughout a distributed system and enforces redundancy and fault tolerance while tracking changes in the system.

The other affected product, RSLinx Enterprise, is used for design and configuration which provides plant-floor device connectivity for multiple Rockwell software applications. It also has open interfaces for third-party human-machine interfaces (HMIs), data collection and analysis packages, as well as custom client-applications.

According to Rockwell Automation, both products are deployed across several sectors including agriculture and food, water, chemical, manufacturing, and others. The Rockwell product Web site states that these products are used in France, Italy, the Netherlands, and other countries in Europe, as well as the United States, Korea, China, Japan, and Latin American countries.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

INTEGER OVERFLOW–NEGATIVE INTEGER[a]

The FactoryTalk Services Platform (RNADiagnostics.dll) does not validate input correctly and cannot allocate a negative integer. By sending a negative integer input to the service over Port 4445/UDP, an attacker could cause a DoS condition that prevents subsequent processing of

a. CWE, http://cwe.mitre.org/data/definitions/190.html, CWE-190: Integer Overflow or Wraparound, Web site last accessed April 05, 2013.

connections. An attacker could possibly cause the RNADiagnostics.dll or RNADiagReceiver.exe service to terminate.

CVE-2012-4713[b] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).[c]

INTEGER OVERFLOW–OVER-SIZED INTEGER[a]

The FactoryTalk Services Platform (RNADiagnostics.dll) does not handle input correctly and cannot allocate an over-sized integer. By sending an over-sized integer input to the service over Port 4445/UDP, an attacker could cause a DoS condition that prevents subsequent processing of connections. An attacker could possibly cause the service to terminate.

CVE-2012-4714[d] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).[e]

IMPROPER EXCEPTION HANDLING[f]

The RSLinx Enterprise Software (LogReceiver.exe and Logger.dll) does not handle input correctly and results in a logic error if it receives a zero byte datagram. If an attacker sends a datagram of zero byte size to the receiver over Port 4444/UDP (user-configurable, not enabled by default), the attacker would cause a DoS condition where the service silently ignores further incoming requests.

CVE-2012-4695[g] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).[h]

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4713 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

c. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C), Web site last visited April 05, 2013.

d. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4714 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

e. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C), Web site last visited April 05, 2013.

f. CWE, http://cwe.mitre.org/data/definitions/703.html, CWE-703: Improper Check or Handling of Exceptional Conditions, Web site last accessed April 05, 2013.

g. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4695, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

h. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C), Web site last visited April 05, 2013.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

BUFFER OVERFLOW[i]

The RSLinx Enterprise Software (LogReceiver.exe and Logger.dll) does not handle input correctly and results in a logic error if it receives a large byte datagram. If an attacker sends a specially crafted datagram of large byte size to the receiver over Port 4444/UDP (user-configurable, not enabled by default), the attacker would cause the LogReceiver.exe service to terminate and have the potential to perform code execution.

CVE-2012-4715[j] has been assigned to this vulnerability. A CVSS v2 base score of 8.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:P/A:C).[k]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with a low skill would be able to exploit these vulnerabilities.

MITIGATION

Rockwell Automation's recommendation to asset owners using FTSP or RSLinx CPR9 through CPR9-SR4 is to upgrade to CPR9-SR5 or newer. Rockwell Automation also recommends that all asset owners using FTSP or RSLinx CPR9-SR5 and newer should apply the correlating patch for the version they are using.

The patches and details pertaining to these vulnerabilities can be found at the following Rockwell Automation Security Advisory link (login is required):

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/537599

i. CWE, http://cwe.mitre.org/data/definitions/120.html, CWE-120: Buffer Copy without Checking Size of Input (Classic Buffer Overflow), Web site last accessed April 05, 2013.

j. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4715, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

k. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:P/A:C), Web site last visited April 05, 2013.

In addition, asset owners can find security information for other Rockwell Automation products at the Security Advisory Index page link below (login is required):

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/54102

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[l] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B—Targeted Cyber Intrusion Detection and Mitigation Strategies,[m] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click Web links or open unsolicited attachments in email messages.

l. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed April 05, 2013.

m. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01B.pdf, Web site last accessed April 05, 2013.

2. Refer to Recognizing and Avoiding Email Scams[n] for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks[o] for more information on social engineering attacks.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.
When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.

I see that this document is labeled as TLP = WHITE. May I distribute this to other people? According to the International Critical Information Infrastructure Protection (CIIP) Traffic Light Protocol[p,q] warning, this document is subject to standard copyright rule and may be distributed freely without restriction.
TLP = WHITE: Unlimited

n. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed Web site last accessed April 05, 2013.
o. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, Web site last accessed Web site last accessed J Web site last accessed April 05, 2013.
p. Traffic Light Protocol—International CIIP Directory, Issue 21, September 2009.
q. US-CERT, http://www.us-cert.gov/tlp/, Web site last accessed April 05, 2013.